IT Security Audit Resources

Purpose: To provide agencies with information regarding identifying resources to conduct Information Technology (IT) Security Audits to meet the requirements of the Commonwealth IT Security Audit Standard, SEC 502-00. Please find a copy of the IT Security Audit Standard at IT Security Audit Standard (SEC502-00) and the IT Security Audit Guideline at: Security Audit Guideline.

IT Security Audit Alternatives - The IT Security Audits required by the *IT Security Audit Standard* (COV ITRM Standard SEC502-00), may be performed by a variety of sources that, in the judgment of the Agency management, have the experience and expertise required to perform IT security audits. These resources may include:

- Agency Internal Auditors,
- Internal Auditors from other agencies in the Agency's Secretariat,
- Internal Auditors from other agencies, states or localities in similar business lines (Example: Lottery IT system auditor from Maryland conducts an IT lottery system audit in Virginia,
- Internal Auditors from other agencies with leave accrued that would allow them to be hired as a wage employee,
- the Auditor of Public Accounts for IT systems they audit,
- the Commonwealth IT Infrastructure Partnership independent auditors for the IT Infrastructure component,
- a private auditing company, or
- staff of a private firm.

Please note that the IT Security Audits should not be performed by the IT Systems Operations staff.

If an agency wishes to contract with a private auditing firm or for IT auditors from the private sector there are two contract methods within the Commonwealth that can be used:

- Supplier Managed Staff Augmentation (SMSA) and
- Advanced IT Resources Contracts.

SMSA is used to contract for an auditor at an hourly rate with the agency providing management of the audit project. The Advance IT Resource Contracts are used to contract for an entire turn key audit including project management with the IT Audit Report as the deliverable. They are both alternatives but have different focuses and processes as follows:

SMSA – An hourly rate based method to augment agency staff on an as-needed basis. Recommended for use when an agency already has existing internal audit management and staff, or the ability to design and manage the audit but needs additional personnel an/or expertise to perform one or more IT Security Audits. The contracted staff person(s) must have their activities thoroughly defined and be closely supervised by agency personnel. Included in this document is guidance that the agency may wish to use to define the level of auditor needed. Contact information for SMSA is:

Cindy Sullivan
110 S. 7th Street, Suite 101
Richmond, VA 23219
Phone: 804-343-3840 Fax: 804-343-3843
E-mail: Cindy_Stonich@compaid.com

Find out more about SMSA here.

Advanced IT Resources Contracts – A contract based on specified deliverables at a set price. Recommended for use in situations where the agency has no audit project management expertise or experience available. The agency may consider using one of the following Advanced IT Resources contracts. Advanced IT Resources are available from various firms under state contract that are able to provide a full range of IT auditing services and consulting including the design and management of the audit in addition to conducting the audit. Included in this document is a template for the agency to use to define the level of auditor needed.

Contact information for **AIT Resources** is as follows:

CGI FEIN#: 54-0856778

CONTRACT VA030815-CGI

Statements of Work:	**Contract Administrator:**
Ben Lewis	Helen Aikman
Phone: (804) 648-3906	Phone: (202) 491-8610
Fax: (804) 648-4317	Fax: (703) 267-2274
E-mail: ben.lewis@cgi.com	E-mail: helen.aikman@cgi.com

BearingPoint FEIN#: 22-3680505

CONTRACT VA030815-BP

Statements of Work:	**Contract Administrator**
Don Parr	Mei-Lei Tsou
Phone: (804) 782–4420	Phone: (804) 782-4428
Fax: (804) 782-4401	Fax: (804) 782-4401
E-mail: dlparr@bearingpoint.net	E-mail: mtsou@bearingpoint.net

CACI FEIN: ##54-1008371

CONTRACT VA030815-CACI

Statements of Work:	**Contract Administrator**
Kristin Downer	Maria Cardenas
Phone: (804) 377-0112	Phone: (703) 679-3419
Fax: (804) 377-0113	Fax: (703) 679-3185
E-mail: kdowner@caci.com	E-mail: mcardenas@caci.com

Northrop Grumman FEIN#: 95-2126773

CONTRACT VA030815-NG

Statements of Work:	**Contract Administrator**
Harrison Jones	Mark Lowe
Phone: (804) 523-1146	Phone: (571) 313-2604
Fax: (804) 864-4984	Fax: (571) 313-2085
E-mail: harrison.jones@ngc.com	E-mail: mark.lowe@ngc.com

Find out more about IT Advanced Resources here.

SUPPLIER MANAGED STAFF AUGMENTATION (SMSA)
STATEMENT OF WORK TEMPLATE

EXHIBIT D
CONTRACT BETWEEN
Agency
AND
Supplier

STATEMENT OF WORK

- This Statement of Work is issued by (Agency) to (Supplier). The objective of the scope of services described in this Statement of Work is for the Supplier to provide the Agency User with "Supplier Managed Staff Augmentation" (SMSA) in the form of qualified auditors and consultants to perform IT Security Auditing and consulting services.

IT AUDITOR QUALIFICATIONS

The augmented staff auditor shall have the skills and knowledge necessary to conduct or assist with the audit assignment. Agencies shall consider the following qualifications when hiring or contracting an IT Security Auditor through an augmented staff contract:

Qualifications of the auditor shall include:

- Graduation from an accredited college or university with major studies in auditing or information systems.
- Progressively responsible experience with IT audits,
- One or more professional credentials such as CISA, CIA, or CPA.

IT AUDITOR INDEPENDENCE

The auditor hired as augmented staff shall be independent in attitude and appearance in all matters related to the audit. In addition, the auditor shall be organizationally independent of the area being audited.

STAFF AUGMENTATION PRICING

Staff augmentation can be provided through state contract # VA-051123-CAI with Computer Aid Incorporated (CAI). The services of audit personnel, if available with CAI, may be obtained at an hourly rate. CAI will provide audit personnel as Senior Consultants at 3 different levels:

Senior Consultant V2 Level 1
Senior Consultant V2 Level 2
Senior Consultant V2 Level 3

Rates are based on zones within the state. Please reference SMSA pricing to get the correct pricing as it relates to the appropriate location (zone).

The level of consultant/auditor that is needed for any particular audit should be determined by the agency based on the level of complexity of the audit project, and the technical expertise required.

1. PROJECT SCOPE AND REQUIREMENTS

1. Perform an IT Security Audit for one or more Sensitive IT System(s) for compliance with the **The audit of the system shall at a minimum assess compliance with** COV ITRM Security Policy SEC500-02, ITRM Security Standard SEC 501-01, and ITRM Security as well as overall adequacy of internal controls.
2. An engagement letter will be developed by the agency to define for the auditor the scope and objectives of the audit. The engagement letter should address the responsibility (scope, independence, deliverables), authority (right of access to information), and accountability (auditees' rights, agreed completion date) of the auditor. Regular status reports should be submitted for tracking progress throughout the course of the engagement.
3. The auditor will conduct the audit in compliance with the IT Security Audit Standard as well as the IT Security Audit Guideline. The agency and the auditor will determine who is accountable for performing the audit preliminary survey phase to include the design of the fieldwork program for testing of internal controls. The auditor shall perform the fieldwork phases as well as the reporting phase under the supervision and project management of agency management. The auditor will ensure that the audit results are supported by work papers with sufficient, competent evidential matter to support the report conclusion. All work papers are the property of the agency Commonwealth of Virginia.
4. Prepare a report to document the conclusions of the review. The final report should include a description of the work that was performed, audit results, recommendations and corrective action plans provided by the agency to include responsible party and dates for completion.

ADDITIONAL CONTRACT SERVICES TO SUPPORT THE REQUIREMENTS

AUDITOR ACCESS

During the all phases of the audit, the auditor will be allowed access to the all applicable information including policies, procedures, work instructions, prior audit reports and personnel with roles related to the IT system being audited.

PERIOD OF PERFORMANCE

The period of performance for Services shall be [start date] to [end date] and may be extended, pursuant to and unless otherwise specified in writing.

PLACE OF PERFORMANCE

Tasks associated with this engagement will be performed at the Agency's location(s) in _____, Virginia, or other locations as required by the effort.

MILESTONES AND DELIVERABLES

The following table identifies milestone events and deliverables for an augmented staff auditor.

Milestone Event	Deliverable	Schedule	Estimated Hrs
Preliminary Review	---	---	
Audit Entrance	Audit Plan	---	

Conference			
Preliminary Survey Internal Control Evaluation	---	---	
Fieldwork Testing Program	----	---	
Potential Management Comments	---	---	
Interim Updates	---	---	
Draft Audit Report	Draft Audit Report	---	
Audit Exit Conference	---	---	
Final Audit Report	Final Audit Report	---	

The total number of hours for augmented staff audit services for the audit engagement shall not exceed XXX hours.

Required Deliverables are as follows:

i). Audit Plan (Scope and Objectives)

ii). Draft Audit Report

iii). Final Audit Report

In addition, the augmented staff auditor will provide copies of any briefing materials, presentations, or other information developed to support this engagement.

Any inventions, combinations, machines, methods, formulae, techniques, processes, improvements, software designs, computer programs, strategies, specific computer-related know-how, data and original works of authorship discovered, created, or developed by the augmented staff auditor, or jointly by the augmented staff auditor and the agency in the execution of this Statement of Work shall be deemed Work Product. Configuration of software shall not be deemed Work Product. All provisions of the Contract regarding Work Product shall apply to this Statement of Work.

Travel expenses incurred by the augmented staff auditor, if any, must be approved in advance by the Agency. Such expenses shall be reimbursed in accordance with Commonwealth of Virginia travel policies as published by the Virginia Department of Accounts.

TESTING AND ACCEPTANCE

Acceptance Criteria for this Solution will be based on the delivery of a final audit report to include corrective action plans.

The Agency IT Sensitive System Business owner or his/her designee (Project Manager) will have ten (10) days from receipt of the deliverable to provide the augmented staff auditor with the signed Acceptance Receipt unless an alternative schedule is mutually agreed to between the auditor and the Authorized User in advance.

Correction of Defects

Correction of defects and Cure Period shall be in accordance with the applicable provisions of the Contract. The auditor shall not be required to correct minor imperfections or defects that do not materially impair the operation or quality of the Deliverable.

SECURITY REQUIREMENTS

Authorized User's security requirements: For any individual agency location, security procedures may include but not be limited to: background checks, records verification, photographing, and fingerprinting of the augmented staff auditor. The auditor may, at any time, be required to execute and complete, additional forms which may include non-disclosure agreements to be signed acknowledging that all agency information with which they may come into contact while at the agency site is confidential and proprietary. Any unauthorized release of proprietary information by the augmented staff auditor shall constitute a breach of the Contract.

At a minimum, all augmented staff auditors shall adhere to all of agency's standard security requirements.

RISK MANAGEMENT

Risk is a function of the probability of an event occurring and the impact of the negative effects if it does occur. Negative effects include schedule delay, increased costs, and poor quality of deliverables.

Depending on the level of risk of this project, as assessed by the agency, this section may contain any or all of the following components, at a level of detail commensurate with the level of risk:

i). Identification of risk factors.

ii). Initial risk assessment.

iii). Risk management/mitigation plan, including determination of roles and responsibilities of the agency and supplier.

iv). Risk monitoring plan, including frequency and form of reviews, project team responsibilities, steering and oversight committee responsibilities, documentation.

REPORTING

Weekly/Bi-weekly Status Update. The weekly/bi-weekly status report, to be submitted by the augmented staff auditor to the agency, should include: accomplishments to date as compared to the project plan; any changes in tasks, resources or schedule with new target dates, if necessary; all open issues or questions regarding the project; action plan for addressing open issues or questions and potential impacts on the project; risk management reporting.

Augmented Auditor Performance Self-Assessment. Within thirty (30) days of execution of the Statement of Work, the augmented staff auditor and the agency will agree on auditor performance self-assessment criteria. The auditor shall prepare a monthly self-assessment to report on such criteria. The auditor shall submit its self-assessment to the agency who will have five (5) days to respond to Supplier with any comments. If the agency agrees with supplier's self-assessment, such agency will sign the self-assessment and submit a copy to the Agency Supplier Relationship Manager.

Augmented Auditor Performance Assessments. The agency may develop assessments of the auditor's performance and disseminate such assessments to other agency's. Prior to dissemination of such assessments, the auditor will have an opportunity to respond to the assessments, and independent verification of the assessment may be utilized in the case of disagreement.

POINT OF CONTACT

For the duration of this project, the following project managers shall serve as the points of contact for day-to-day communication:

Agency: _____

Supplier: _____

This Statement of Work is issued pursuant to and, upon execution, shall become an incorporated exhibit to the Contract. In the event of conflict, the following order of precedence shall apply:

i). The Contract

ii). This Exhibit D

By signing below, both parties agree to the terms of this Exhibit.

Supplier	Agency
By: _____	By: _____
(Signature)	(Signature)
Name: _____	Name: _____
(Print)	(Print)
Title: _____	Title: _____
Date: _____	Date: _____

ADVANCED IT RESOURCES
STATEMENT OF WORK TEMPLATE

EXHIBIT D-X
CONTRACT NUMBER VA-000000-XXXX
BETWEEN
VIRGINIA INFORMATION TECHNOLOGIES AGENCY
AND
Supplier

Exhibit D-X is hereby incorporated into and made an integral part of Contract Number VA-000000-XXXX ("Contract") between the agency ("AGENCY" or "Commonwealth" or "State") and supplier ("supplier").
In the event of any discrepancy between this Exhibit D-X and Contract No. VA-000000-XXXX, the provisions of Contract No. VA-000000-XXXX shall control.

STATEMENT OF WORK

This Statement of Work is issued by VITA on behalf of Authorized User (agency), hereinafter referred to as "Authorized User". The objective of the project described in this Statement of Work is for the supplier to provide the Authorized User with IT Security Auditing and consulting services ("Services"). For information on how to obtain services under this contract, click here.

SUPPLIER QUALIFICATIONS

- The supplier shall have resources available with the skills and knowledge necessary to perform project management oversight as well as conduct the audit assignment. Preferred supplier qualifications would include a proven track record in successfully performing IT Security Audit projects. The supplier shall demonstrate the use of best practices and industry accepted frameworks in meeting the requirements for IT Security Auditing and Project Management. Best practices and frameworks recommended may include NIST, COBIT, ITIL, and Project Management Institute.

  Qualifications of the auditor assigned shall include:

  - Graduation from an accredited college or university with major studies in auditing or information systems,
  - Progressively responsible experience with IT audits, and
  - One or more professional credentials such as CISA, CIA, or CPA.

IT AUDITOR INDEPENDENCE

The auditing firm and assigned staff shall be independent in attitude and appearance in all matters related to the audit. In addition, the auditor should be organizationally independent of the area being audited.

PROJECT SCOPE AND REQUIREMENTS

1. Perform an IT Security Audit for one or more Sensitive IT System(s)) for compliance with the **The audit of the system shall at a minimum assess compliance with** COV ITRM Security Policy SEC500-02, ITRM Security Standard SEC 501-01, and ITRM Security as well as overall adequacy of internal controls.

2. An engagement letter will be developed by the Agency to define for the auditor the scope and objectives of the audit. The engagement letter should address the responsibility (scope, independence, deliverables), authority (right of access to information), and accountability (auditees' rights, agreed completion date) of the auditor.

3. The firm will be required to perform a preliminary review of the IT system(s) or function(s) to be audited, assess risks, and to evaluate the agency's internal controls to provide reasonable assurance that: sensitive data and IT assets are safeguarded; operations are effective and efficient; management information is reliable and complete and that compliance is achieved with applicable laws and regulations.

4. The firm will be expected to design and administer all aspects of the audit and ensure the audit is conducted in compliance with the IT Security Audit Standard as well as the IT Security Audit Guideline. The firm shall conduct all phases of the audit including familiarization, preliminary survey, fieldwork, reporting as well as all project management to ensure that the audit report is on-time, accurate, reliable and supported by work papers with sufficient, competent evidential matter to support the report conclusion. All work papers are the property of the agency Commonwealth of Virginia.

4. Prepare a report to document the conclusions of the review. The final report should include a description of the work that was performed, audit results, recommendations and corrective action plans provided by the agency to include responsible party and dates for completion.

ADDITIONAL CONTRACT SERVICES TO SUPPORT THE REQUIREMENTS

AUDITOR ACCESS

During the all phases of the audit, the auditor will be allowed access to the all applicable information including policies, procedures, work instructions, prior audit reports and personnel with roles related to the IT system being audited.

PERIOD OF PERFORMANCE

The period of performance for Services shall be [start date] to [end date] and may be extended, pursuant to and unless otherwise specified in writing.

PLACE OF PERFORMANCE

Tasks associated with this engagement will be performed at the Authorized User's location(s) in _____, Virginia, at supplier's location(s) in Wherever, or other locations as required by the effort.

MILESTONES, DELIVERABLES, PAYMENT SCHEDULE, AND HOLDBACKS

The following table identifies milestone events and deliverables, the associated schedule, any associated payments, any retainage amounts, and net payments.

Milestone Event	Deliverable	Schedule	Payment	Retainage	Net Payment

Preliminary Review	---	---	---	---	---
Audit Entrance Conference	Audit Plan	---	---	---	---
Preliminary Survey Internal Control Evaluation	---	---	---	---	---
Fieldwork Testing Program	----	----	---	---	---
Potential Management Comments	---	---	---	---	---
Interim Updates	---	---	---	---	---
Draft Audit Report	Draft Audit Report	---	---	---	---
Audit Exit Conference	---	---	---	---	---
Final Audit Report	Final Audit Report	---	---	---	---

The total price for Services shall not exceed $US XXX.

Supplier's invoices shall show retainage of ten percent (10%). Following completion of Services, Supplier shall submit a final invoice to the Authorized User, for the final milestone payment amount plus the total amount retained by the Authorized User.

Required Deliverables are as follows:

i). Audit Plan (Scope and Objectives)

ii). Draft Audit Report

iii). Final Audit Report

In addition, supplier will provide copies of any briefing materials, presentations, or other information developed to support this engagement.

Any inventions, combinations, machines, methods, formulae, techniques, processes, improvements, software designs, computer programs, strategies, specific computer-related know-how, data and original works of authorship discovered, created, or developed by supplier, or jointly by supplier and an Authorized User(s) in the execution of this Statement of Work shall be deemed Work Product. Configuration of software shall not be deemed Work Product. All provisions of the Contract regarding Work Product shall apply to this Statement of Work.

If travel expenses are not included in the fixed price of the solution, such expenses shall be reimbursed in accordance with Commonwealth of Virginia travel policies as published by the Virginia Department of Accounts.

TESTING AND ACCEPTANCE

Acceptance criteria for this solution will be based on the delivery of a final audit report to include corrective action plans.

The Agency IT Sensitive System Business owner or his/her designee (Project Manager) will have ten (10) days from receipt of the deliverable to provide supplier with the signed Acceptance Receipt unless an alternative schedule is mutually agreed to between supplier and the Authorized User in advance.

Correction of Defects

Correction of defects and Cure Period shall be in accordance with the applicable provisions of the contract. Supplier shall not be required to correct minor imperfections or defects that do not materially impair the operation or quality of the deliverable.

SECURITY REQUIREMENTS

Authorized User's security requirements. For any individual Authorized User location, security procedures may include but not be limited to: background checks, records verification, photographing, and fingerprinting of Supplier's employees or agents. Supplier may, at any time, be required to execute and complete, for each individual Supplier employee or agent, additional forms which may include non-disclosure agreements to be signed by supplier's employees or agents acknowledging that all Authorized User information with which such employees and agents come into contact while at the Authorized User site is confidential and proprietary. Any unauthorized release of proprietary information by the Supplier or an employee or agent of supplier shall constitute a breach of the contract.

At a minimum, supplier shall adhere to all of AGENCY's standard security requirements.

RISK MANAGEMENT

Risk is a function of the probability of an event occurring and the impact of the negative effects if it does occur. Negative effects include schedule delay, increased costs, and poor quality of deliverables.

Depending on the level of risk of this project, as assessed by the Authorized User, this section may contain any or all of the following components, at a level of detail commensurate with the level of risk:

i). Identification of risk factors.

ii). Initial risk assessment.

iii). Risk management/mitigation plan, including determination of roles and responsibilities of the Authorized User and supplier.

iv). Risk monitoring plan, including frequency and form of reviews, project team responsibilities, steering and oversight committee responsibilities, and documentation.

REPORTING

Weekly/Bi-weekly Status Update. The weekly/bi-weekly status report, to be submitted by supplier to the Authorized User, should include: accomplishments to date as compared to the project plan; any changes in tasks, resources or schedule with new target dates, if necessary; all open issues or questions regarding the project; action plan for addressing open issues or questions and potential impacts on the project; risk management reporting.

Supplier Performance Self-Assessment. Within thirty (30) days of execution of the Statement of Work, the Supplier and the Authorized User will agree on supplier performance self-assessment criteria. Supplier shall prepare a monthly self-assessment to report on such criteria. Supplier shall submit its self-assessment to the Authorized

User who will have five (5) days to respond to supplier with any comments. If the Authorized User agrees with supplier's self-assessment, such Authorized User will sign the self-assessment and submit a copy to the AGENCY Supplier Relationship Manager.

Supplier Performance Assessments. The Authorized User may develop assessments of the supplier's performance and disseminate such assessments to other Authorized Users of the Contract. Prior to dissemination of such assessments, supplier will have an opportunity to respond to the assessments, and independent verification of the assessment may be utilized in the case of disagreement.

POINT OF CONTACT

For the duration of this project, the following project managers shall serve as the points of contact for day-to-day communication:

Authorized User: _____

Supplier: _____

This Statement of Work is issued pursuant to and, upon execution, shall become an incorporated exhibit to the Contract. In the event of conflict, the following order of precedence shall apply:

i). The Contract

ii). This Exhibit D-X

By signing below, both parties agree to the terms of this Exhibit.

Supplier	Authorized User
By: _____	By: _____
(Signature)	(Signature)
Name: _____	Name: _____
(Print)	(Print)
Title: _____	Title: _____
Date: _____	Date: _____